

1 Joshua B. Swigart (SBN 225557)  
2 *josh@swigartlawgroup.com*  
3 **SWIGART LAW GROUP, APC**  
4 2221 Camino Del Rio S., Suite 308  
5 San Diego, CA 92108  
6 Tel: (866) 219-3343; Fax: (866) 219-8344

7 Ben Travis (SBN 305641)  
8 *ben@bentravislaw.com*  
9 **BEN TRAVIS LAW, APC**  
10 4660 La Jolla Village Drive, Suite 100  
11 San Diego, CA 92122  
12 Phone: (619) 353-7966

13 *Additional counsel listed on signature page*

14 Attorneys for Plaintiff Andrew Rose  
15 and the putative class

16  
17 **UNITED STATES DISTRICT COURT**  
18 **CENTRAL DISTRICT OF CALIFORNIA**  
19

20 ANDREW ROSE, an individual, on  
21 behalf of himself and all others  
22 similarly situated,

23 Plaintiff,

24 v.

25 INTERNATIONAL BUSINESS  
26 MACHINES CORPORATION; and  
27 JOHNSON & JOHNSON HEALTH  
28 CARE SYSTEMS, INC.,

Defendants.

Case No.:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

**CLASS ACTION**

1 Plaintiff ANDREW ROSE (“Plaintiff”), by and through his attorneys, brings this  
2 class action on behalf of himself, and the Class, as defined below, against Defendants  
3 INTERNATIONAL BUSINESS MACHINES CORPORATION (“IBM”) and  
4 JOHNSON & JOHNSON HEALTH CARE SYSTEMS INC. (“JANSSEN”)  
5 (collectively “Defendants”). Plaintiff hereby alleges, on information and belief, except  
6 for information based on personal knowledge, which allegations are likely to have  
7 evidentiary support after further investigation and discovery, as follows:

### 8 **INTRODUCTION**

9 1. Plaintiff brings this Class Action because of Defendants’ failures to  
10 properly secure and safeguard individuals’ sensitive personal data.

11 2. Defendant JANSSEN provides business support services to large health  
12 care clients, as well as access to parent Johnson & Johnson’s products. Its  
13 customers include managed care organizations, hospital groups, physician networks,  
14 pharmacies, and government customers. The company also provides e-business and  
15 supply management services for a number of fellow Johnson & Johnson subsidiaries.

16 3. JANSSEN utilizes a platform called JANSSEN CarePath, which is a  
17 patient support platform that offers savings options and other patient support resources.

18 4. Defendant IBM is a multinational technology company that  
19 provides infrastructure, software and consulting services for clients.

20 5. IBM is a service provider to Defendant JANSSEN and manages the  
21 application and the third-party database that supports Janssen CarePath.

22 6. Plaintiff and all other persons similarly situated had a right to keep their  
23 Personally Identifiable Information (“PII”) maintained by Defendants confidential (the  
24 PII maintained by Defendants is collectively referred to as “Sensitive Information”).  
25 Plaintiff and other members of the Class relied on Defendants to keep their Sensitive  
26 Information confidential as required by the applicable laws.

27 7. Defendants violated this right. They failed to implement or follow  
28 reasonable data security procedures as required by law and failed to protect Plaintiff

1 and the proposed Class members' Sensitive Information from unauthorized access.

2 8. As a result of Defendants' inadequate data security and inadequate or  
3 negligent training of their employees, Plaintiff's and other proposed Class members'  
4 Sensitive Information, including confidential medical information, was accessed and  
5 taken by unauthorized third parties. ("Data Breach").

6 9. While Defendants learned of the breach on August 2, 2023, they waited  
7 till September 29, 2023 to notify Plaintiff and other Class members.

8 10. The Data Breach was a direct result of Defendants' failures to implement  
9 adequate and reasonable cybersecurity procedures and protocols necessary to protect  
10 Plaintiff's and other Class members' Sensitive Information.

11 11. Defendants disregarded the rights of Plaintiff and Class members by,  
12 among other things, recklessly or negligently failing to take adequate and reasonable  
13 measures to ensure their data systems were protected against unauthorized intrusions;  
14 failing to disclose that they did not have reasonable or adequately robust computer  
15 systems and security practices to safeguard Sensitive Information; failing to take  
16 standard and reasonably available steps to prevent the Data Breach; failing to monitor  
17 and timely detect the Data Breach; and failing to provide Plaintiff and Class members  
18 prompt and accurate notice of the Data Breach.

19 12. As a result of Defendants' failures to implement and follow reasonable  
20 security procedures, Class members' Sensitive Information is now exposed. Plaintiff  
21 and Class members have spent, and will continue to spend, significant amounts of time  
22 and money trying to protect themselves from the adverse ramifications of the Data  
23 Breach and dealing with actual fraud and will forever be at a heightened risk of identity  
24 theft and fraud.

25 13. Plaintiff, on behalf of himself and all others similarly situated, alleges  
26 claims for (1) violation of the California Confidentiality of Medical Information Act  
27 ("CMIA") (Cal. Civ. Code § 56 *et seq.*); (2) negligence; (3) invasion of privacy;  
28 (4) breach of implied contract; (5) breach of fiduciary duty; (6) breach of confidence;

1 (7) violation of the California Unfair Competition Law (Cal. Business & Professions  
2 Code § 17200, *et seq.*); (8) violation of the California Customer Records Act  
3 (“CCRA”) (Cal. Civ. Code § 1798.80, *et seq.*), and (9) violations of the California  
4 Consumer Privacy Act (“CCPA”) (Cal. Civ. Code § 1798.150, *et seq.*). Plaintiff and  
5 the Class members seek damages, including but not limited to nominal damages from  
6 Defendants, and to compel Defendants to adopt reasonably sufficient security practices  
7 to safeguard Sensitive Information that remains in Defendants’ custody to prevent  
8 incidents like the Data Breach from reoccurring in the future.

### 9 **JURISDICTION AND VENUE**

10 14. This Court has personal jurisdiction over Defendants because Defendants  
11 conduct substantial business in California and are registered to do business in  
12 California.

13 15. This court has subject matter jurisdiction pursuant to the Class Action  
14 Fairness Act, 28 U.S.C. 1332(d), as Plaintiff and Defendants are diverse, there are over  
15 100 Class members, and the amount in controversy exceeds \$5 million.

16 16. Venue is proper in this Court because a substantial portion of the acts  
17 giving rise to this action occurred in this District.

### 18 **PARTIES**

19 17. Plaintiff is an individual over the age of eighteen years, and at all times  
20 relevant herein was and is, a resident of the County of Ventura in the State of California.

21 18. Defendant IBM is a New York corporation with its principal place of  
22 business also in New York.

23 19. Defendant JANSSEN is a New Jersey corporation with its principal place  
24 of business also in New Jersey.

### 25 **FACTUAL ALLEGATIONS**

#### 26 **A. Background**

27 20. Defendant JANSSEN provides business support services to large health  
28 care clients, as well as access to parent Johnson & Johnson's products. Its

1 customers include managed care organizations, hospital groups, physician networks,  
2 pharmacies, and government customers. The company also provides e-business and  
3 supply management services for a number of fellow Johnson & Johnson subsidiaries.

4 21. JANSSEN utilizes a platform called JANSSEN CarePath, which is a  
5 patient support platform that offers savings options and other patient support resources.

6 22. Defendant IBM is a service provider to Defendant JANSSEN. IBM  
7 manages the application and the third-party database that supports Janssen CarePath.

8 23. As part of their business, Defendants store a vast amount of Sensitive  
9 Information. In doing so, Defendants were entrusted with, and obligated to safeguard  
10 and protect, the Sensitive Information of Plaintiff and the Class in accordance with all  
11 applicable laws.

12 **B. The Data Breach**

13 24. On or around September 29, 2023, Defendants issued a Notice of Data  
14 Breach notifying consumers of an incident involving unauthorized access to personal  
15 information (“September 2023 Data Breach Notice”). The September 2023 Data  
16 Breach Notice informed the affected members that Defendants recently became aware  
17 of a technical method by which unauthorized access to the database could be obtained.  
18 Defendants allegedly undertook an investigation to assess whether there had been  
19 unauthorized access to the database. On August 2, 2023, they determined that there  
20 was unauthorized access to personal information in the database but were unable to  
21 determine the scope of the access.

22 25. The September 2023 Data Breach Notice identified the following data  
23 points involved: name, contact information, health insurance information, and  
24 information about medications and associated conditions that were provided to the  
25 Janssen CarePath application.

26 26. Defendants failed to put in place proper security protocols to protect  
27 against the unauthorized release of consumers’ information and failed to properly train  
28 their employees on such protocols, resulting in the unauthorized release of private data.

1 As a result of Defendants' failures, Plaintiff and the Class members' Sensitive  
2 Information was accessed and viewed by unknown and unauthorized third parties and  
3 is available on the dark web. This means that the Data Breach was successful:  
4 unauthorized individuals accessed Plaintiff's and the Class members' unencrypted,  
5 unredacted information set forth above.

6 27. Plaintiff received the September 2023 Data Breach Notice from Defendant  
7 IBM on or about September 29, 2023, informing him of the Data Breach and that his  
8 Sensitive Information was present in the affected systems. The Data Breach  
9 notification indicated the following information may have been compromised: name,  
10 contact information, health insurance information, and information about medications  
11 and associated conditions that were provided to the Janssen CarePath application.

12 28. This kind of Sensitive Information is highly valued by criminals, as  
13 evidenced by the prices they will pay through the dark web. For example, personal  
14 information can be sold at a price ranging from \$40 to \$200.

### 15 **C. Plaintiff's Exposure**

16 29. Knowing that thieves stole his Sensitive Information and knowing that his  
17 Sensitive Information may now or in the future be available for sale on the dark web  
18 has caused Plaintiff great anxiety. He is now very concerned about fraud and identity  
19 theft.

20 30. Plaintiff suffered actual injury from having his Sensitive Information  
21 exposed as a result of the Data Breach including, but not limited to: (a) damages to  
22 and diminution in the value of his Sensitive Information—a form of intangible property  
23 that Plaintiff entrusted to Defendants; (b) loss of his privacy; (c) imminent and  
24 impending injury arising from the increased risk of fraud and identity theft; and (d) the  
25 time and expense of mitigation efforts as a result of the Data Breach.

26 31. As a result of the Data Breach, Plaintiff will continue to be at heightened  
27 risk for financial fraud, and identity theft, and the attendant damages, for years to come.

28 32. Defendants' failure to provide immediate formal notice of the Breach to

1 Plaintiff and Class members exacerbated the injuries resulting from the Breach.

2 **D. Defendants Knew or Should Have Known of the Risk Because Medical**  
3 **Providers are Particularly Susceptible to Cyber Attacks.**

4 33. The number of U.S. data breaches surpassed 1,000 in 2016—a record high  
5 and a 40 percent increase in the number of data breaches from the previous year.<sup>1</sup> In  
6 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in  
7 just one year.<sup>2</sup> That trend continues.

8 34. Medical information is especially valuable to identity thieves. Because of  
9 its value, the medical industry has experienced disproportionately higher numbers of  
10 data theft events than other industries. Defendants knew or should have known this  
11 and strengthened their data systems accordingly. Defendants were put on notice of the  
12 substantial and foreseeable risk of harm from a data breach, yet they failed to properly  
13 prepare for that risk.

14 35. Defendants knew and understood that unprotected or exposed Sensitive  
15 Information in the custody of medical providers, such as Defendants, is valuable and  
16 highly sought after by nefarious third parties seeking to illegally monetize that  
17 Sensitive Information through unauthorized access. Indeed, when compromised,  
18 highly confidential related data is among the most sensitive and personally  
19 consequential. Data breaches and identity theft have a crippling effect on individuals,  
20 and detrimentally impacts the economy as a whole.

21 36. Defendants knew, or should have known, the importance of safeguarding  
22

---

23 <sup>1</sup> Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds*  
24 *New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017),  
25 available at: [https://www.prnewswire.com/news-releases/data-breaches-increase-40-](https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html)  
26 [percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-](https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html)  
[cyberscout-300393208.html](https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html) (last accessed October 17, 2023).

27 <sup>2</sup> Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*,  
28 available at:

[https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreach](https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf)  
[YearEndReview.pdf](https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf) (last accessed October 17, 2023).

1 Sensitive Information entrusted to them by Plaintiff and Class members, and of the  
2 foreseeable consequences if their data security systems were breached. This includes  
3 the significant costs imposed on Plaintiff and Class members as a result of a breach.  
4 Defendants failed, however, to take adequate cybersecurity measures to prevent the  
5 Data Breach.

6 **E. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII.**

7 37. Defendants acquire, collect, and store a massive amount of consumers'  
8 protected confidential information and other personally identifiable data.

9 38. As a condition of providing services, Defendants require consumers to  
10 entrust them with highly confidential Sensitive Information.

11 39. By requiring, obtaining, collecting, using, and deriving a benefit from  
12 Plaintiff's and Class members' Sensitive Information, Defendants assumed legal and  
13 equitable duties, and knew or should have known they were responsible for protecting  
14 Plaintiff's and Class members' Sensitive Information from disclosure.

15 40. Plaintiff and Class members have taken reasonable steps to maintain the  
16 confidentiality of their Sensitive Information. Plaintiff and Class members relied on  
17 Defendants to keep their Sensitive Information confidential and securely maintained,  
18 to use this information for business purposes only, to only allow authorized disclosures  
19 of this information, and prevent unauthorized disclosure of the information.

20 **F. The Value of PII and the Effects of Unauthorized Disclosure.**

21 41. Defendants were well aware of the highly private nature of the Sensitive  
22 Information they collect and its significant value to those who would use it for wrongful  
23 purposes.

24 42. Sensitive Information is a valuable commodity to identity thieves. As the  
25 FTC recognizes, identity thieves can commit an array of crimes including identify theft,  
26 medical fraud, and financial fraud.<sup>3</sup> Indeed, a robust "cyber black market" exists in  
27

28 <sup>3</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at:  
<https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last

1 which criminals openly post stolen PII on multiple underground Internet websites,  
2 commonly referred to as the dark web.

3 43. The ramifications of Defendants' failure to keep Plaintiff's and Class  
4 members' Sensitive Information secure are long lasting and severe. Once Sensitive  
5 Information is stolen, fraudulent use of that information and damage to victims may  
6 continue for years.

7 44. At all relevant times, Defendants knew, or reasonably should have known,  
8 of the importance of safeguarding Sensitive Information and of the foreseeable  
9 consequences if their data security systems were breached, including the significant  
10 costs that would be imposed on consumers as a result of a breach.

11 **G. Defendants Failed to Comply with FTC Guidelines.**

12 45. The Federal Trade Commission ("FTC") promulgates numerous guides for  
13 businesses highlighting the importance of implementing reasonable data security  
14 practices. According to the FTC, the need for data security should be factored into all  
15 business decision-making.<sup>4</sup>

16 46. In 2016, the FTC updated its publication, *Protecting Personal Information:*  
17 *A Guide for Business*, which established cybersecurity guidelines for businesses.<sup>5</sup> The  
18 guidelines note that businesses should protect the personal customer information they  
19 keep; properly dispose of personal information that is no longer needed; encrypt  
20 information stored on computer networks; understand their network's vulnerabilities;  
21 and implement policies to correct any security problems.

22 47. The FTC further recommends companies not maintain PII longer than is  
23

24 \_\_\_\_\_  
accessed October 17, 2023).

25 <sup>4</sup> Federal Trade Commission, *Start With Security*, available at:  
26 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-  
startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed October 17, 2023).

27 <sup>5</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for*  
28 *Business*, available at [https://www.ftc.gov/system/files/documents/plain-  
language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed October 17,  
2023).

1 needed for authorization of a transaction; limit access to sensitive data; require complex  
2 passwords to be used on networks; use industry-tested methods for security; monitor  
3 for suspicious activity on the network; and verify third-party service providers have  
4 implemented reasonable security measures.<sup>6</sup>

5 48. The FTC brings enforcement actions against businesses for failing to  
6 adequately and reasonably protect customer data, treating the failure to employ  
7 reasonable and appropriate measures to protect against unauthorized access to  
8 confidential consumer data as an unfair act or practice prohibited by Section 5 of the  
9 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these  
10 actions further clarify the measures businesses must take to meet their data security  
11 obligations.

12 49. Defendants failed to properly implement basic data security practices.  
13 Defendants’ failures to employ reasonable and appropriate measures to protect against  
14 unauthorized access to consumers’ Sensitive Information constitutes an unfair act or  
15 practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

16 50. Defendants were at all times fully aware of their obligations to protect  
17 Plaintiff’s and Class members’ Sensitive Information because of Defendant  
18 JANSSEN’s position as a trusted and experienced medical provider and Defendant  
19 IBM’s position as a trusted and experienced technology company. Defendants were  
20 also aware of the significant repercussions that would result from their failures to do  
21 so.

#### 22 **H. Defendants Failed to Comply with Industry Standards.**

23 51. Defendants failed to implement several basic cybersecurity safeguards that  
24 can be implemented to improve cyber resilience and require a relatively small financial  
25 investment yet can have a major impact on an organization’s cybersecurity posture  
26 including: (a) the proper encryption of PII; (b) educating and training employees on  
27 how to protect PII; and (c) correcting the configuration of software and network  
28

---

<sup>6</sup> FTC, *Start With Security*, *supra*.

1 devices.

2 52. Private cybersecurity firms have also identified businesses as being  
3 particularly vulnerable to cyber-attacks, both because of the value of the PII they  
4 maintain and because employees have been slow to adapt and respond to cybersecurity  
5 threats.<sup>7</sup> These private cybersecurity firms have also promulgated similar best practices  
6 for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

7 53. Despite the abundance and availability of information regarding the threats  
8 and cybersecurity best practices to defend against those threats, Defendants chose to  
9 ignore them. These best practices were known, or should have been known by  
10 Defendants, whose failure to heed and properly implement industry standards directly  
11 led to the Data Breach and the unlawful exposure of Sensitive Information.

12 **I. Defendants Failed to Comply with HIPAA.**

13 54. Under the Health Insurance Portability Act of 1996 (“HIPAA”) Defendants  
14 had a heightened duty to protect patient Private Information.

15 55. Defendants failed to comply with HIPAA by not:

- 16 a. Ensuring the confidentiality and integrity of electronic protected health  
17 information (“PHI”) they created, received, maintained, and/or  
18 transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- 19 b. Implementing technical policies and procedures for electronic information  
20 systems that maintain electronic PHI to allow access only to those persons  
21 or software programs that have been granted access rights in violation of  
22 45 C.F.R. § 164.312(a)(1);
- 23 c. Implementing policies and procedures to prevent, detect, contain, and  
24 correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- 25 d. Implementing procedures to review records of information system activity

---

26  
27 <sup>7</sup> Stickman Cyber, *Why Cybersecurity In The Workplace Is Everyone’s*  
28 *Responsibility*, available at: [https://www.stickmancyber.com/cybersecurity-  
blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility](https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility) (last accessed  
October 17, 2023).

regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

- e. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- f. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- g. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or
- h. Training all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

**J. Plaintiff and Class Members Suffered Damages.**

56. The ramifications of Defendants' failures to keep Plaintiff's and Class members' Sensitive Information secure are long lasting and severe. Once that kind of Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

57. The Sensitive Information belonging to Plaintiff and Class members is private, sensitive in nature, and left inadequately protected by Defendants—who did not obtain Plaintiff's or Class members' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

58. The Data Breach was a direct and proximate result of Defendants' failures to: (a) properly safeguard and protect Plaintiff's and Class members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the

1 security and confidentiality of Plaintiff's and Class members' Sensitive Information;  
2 and (c) protect against reasonably foreseeable threats to the security or integrity of such  
3 information.

4 59. Defendants had the resources necessary to prevent the Data Breach, but  
5 neglected to adequately implement data security measures, despite their obligations to  
6 protect member data.

7 60. Defendants could have prevented the intrusions into their systems and,  
8 ultimately, the theft of Sensitive Information if Defendants had remedied the  
9 deficiencies in their data security systems and adopted security measures recommended  
10 by experts in the field.

11 61. As a direct and proximate result of Defendants' wrongful actions and  
12 inactions, Plaintiff and Class members are now in imminent, immediate, and  
13 continuing increased risk of harm from identity theft and fraud, requiring them to  
14 dedicate time and resources which they otherwise would have dedicated to other life  
15 demands, such as work and family, to mitigate the actual and potential impact of the  
16 Data Breach on their lives.

17 62. The U.S. Department of Justice's Bureau of Justice Statistics found that  
18 "among victims who had personal information used for fraudulent purposes, 29% spent  
19 a month or more resolving problems," and that "resolving the problems caused by  
20 identity theft may take more than a year for some victims."<sup>8</sup>

21 63. As a direct result of the Defendants' failures to prevent the Data Breach,  
22 Plaintiff and Class members have suffered, will suffer, and are at increased risk of  
23 suffering:

- 24 a. The compromise, publication, theft and/or unauthorized use of their  
25 Sensitive Information;

---

27 <sup>8</sup> U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics,  
28 *Victims of Identity Theft*, 2012, December 2013, available at:  
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed October 17, 2023).

- b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;
- d. The continued risk to their Sensitive Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Sensitive Information in their possession; and
- e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

64. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

**K. Defendants' Delay in Identifying & Reporting the Breach Caused Additional Harm.**

65. It is axiomatic that:

The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.<sup>9</sup>

---

<sup>9</sup> *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16*

1       66. Indeed, once a data breach has occurred:

2       [o]ne thing that does matter is hearing about a data breach quickly. That  
3       alerts consumers to keep a tight watch on credit card bills, insurance  
4       invoices, and suspicious emails. It can prompt them to change passwords  
5       and freeze credit reports. And notifying officials can help them catch  
6       cybercriminals and warn other businesses of emerging dangers. If  
7       consumers don't know about a breach because it wasn't reported, they  
8       can't take action to protect themselves (internal citations omitted).<sup>10</sup>

9       67. Although their Sensitive Information was improperly exposed on or before  
10      August 2, 2023, Plaintiff and Class members were not notified of the Data Breach until  
11      on or about September 29, 2023, depriving Plaintiff and Class members of the ability  
12      to promptly mitigate potential adverse consequences resulting from the Data Breach.

13      68. As a result of Defendants' delay in detecting and notifying consumers of  
14      the Data Breach, there is an increased risk of fraud for Plaintiff and Class members.

15                                   **CLASS ACTION ALLEGATIONS**

16      69. Plaintiff brings this class action pursuant to Rule 23(a) and (b)(3) of the  
17      Federal Rules of Civil Procedure, on behalf of the following Class and Subclass:

18  
19      All individuals whose Sensitive Information stored or possessed by  
20      Defendants was subject to the Data Breach (the "Class").  
21  
22

23  
24      \_\_\_\_\_  
25      *Percent According to New Javelin Strategy & Research Study*, Business Wire,  
26      *available at:* <https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million> (last accessed October 17, 2023).

27      <sup>10</sup> Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit*  
28      *giants like Equifax and Marriott. Breaches at small companies put consumers at risk,*  
    *too*, January 31, 2019, *available at:* <https://www.consumerreports.org/data-theft/the-data-breach-next-door/> (last accessed October 17, 2023).

1 All California residents whose Sensitive Information stored or  
2 possessed by Defendants was subject to the Data Breach  
3 (the “California Subclass”).

4  
5 70. Excluded from the Class are Defendants, their officers and directors,  
6 families and legal representatives, heirs, successors, or assigns and any entity in which  
7 Defendants have a controlling interest, and any Judge assigned to this case and their  
8 immediate families.

9 71. Plaintiff reserves the right to amend or modify the definition of the Class  
10 and Subclass to provide greater specificity and/or further division into subclasses or  
11 limitation to particular issues.

12 72. **Numerosity- Fed. R. Civ. P. 23(a)(1):** The members of the Class are so  
13 numerous that joinder of all members is impracticable. The exact number or  
14 identification of class members is presently unknown, but it is believed that there are  
15 thousands of class members in the Class. The identities of the Class Members are  
16 ascertainable and can be determined based on records maintained by Defendants.

17 73. **Predominance of Common Questions- Fed R. Civ. P. 23(a)(2),**  
18 **23(b)(3):** There are multiple questions of law and fact common to the Class that will  
19 predominate over questions affecting only individual class members. The questions of  
20 fact and law that are common to the Class members and predominate over questions  
21 that may affect individual Class members, include:

- 22 a) Whether Plaintiff’s and the Class members’ Sensitive Information was  
23 accessed and/or viewed by one or more unauthorized persons in the Data  
24 Breach alleged above;
- 25 b) When and how Defendants should have learned and actually learned of  
26 the Data Breach;
- 27 c) Whether Defendants’ response to the Data Breach was adequate;
- 28 d) Whether Defendants owed a duty to the Class to exercise due care in

collecting, storing, safeguarding and/or obtaining their Sensitive Information;

- e) Whether Defendants breached that duty;
- f) Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' Sensitive Information;
- g) Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' Sensitive Information;
- h) Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class members' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;
- i) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j) Whether Defendants caused Plaintiff and Class members damages;
- k) Whether Defendants violated the law by failing to promptly notify Class members that their Sensitive Information was compromised;
- l) Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief;
- m) Whether Defendants violated the California Unfair Competition Law (Business & Professions Code § 17200, et seq.);
- n) Whether Defendants violated the California Customer Records Act (Cal. Civ. Code § 1798.80, et seq.);
- o) Whether Defendants violated the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100, et seq.).

74. **Typicality- Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class members because all had their Sensitive Information compromised

1 because of the Data Breach, due to Defendants’ virtually identical conduct.

2 75. **Adequacy—Fed. R. Civ. P. 23(a)(4); 23(g)(1):** Plaintiff is an adequate  
3 representative of the Class because he is a member of the Class and his interests do not  
4 conflict with the interests of the members of the Class he seeks to represent. Plaintiff  
5 is represented by experienced and competent Class Counsel. Class Counsel have  
6 litigated numerous class actions. Class counsel intend to prosecute this action  
7 vigorously for the benefit of everyone in the Class. Plaintiff and Class Counsel can  
8 fairly and adequately protect the interests of all of the members of the Class.

9 76. **Superiority—Fed. R. Civ. P. 23(b)(3):** The class action is superior to  
10 other available methods for fairly and efficiently adjudicating this controversy because  
11 individual litigation of Class members’ claims would be impracticable and individual  
12 litigation would be unduly burdensome to the courts. Without the class action vehicle,  
13 the Class would have no reasonable remedy and would continue to suffer losses.  
14 Further, individual litigation has the potential to result in inconsistent or contradictory  
15 judgments. There is no foreseeable difficulty in managing this action as a class action  
16 and it provides the benefits of single adjudication, economies of scale, and  
17 comprehensive supervision by a single court.

18 **First Cause of Action**

19 **Violation of California’s Confidentiality of**  
20 **Medical Information Act (“CMIA”)**

21 **(Cal. Civ. Code § 56, et seq.)**

22 **[On Behalf of Plaintiff and the California Subclass Against all Defendants]**

23 77. Plaintiff re-alleges and incorporates by reference each and every allegation  
24 contained in the preceding and subsequent paragraphs as though fully set forth herein.

25 78. Defendants are “provider[s] of healthcare,” as defined in Cal. Civ. Code §  
26 56.06 and/or a “contractor,” and are therefore subject to the requirements of the CMIA,  
27 Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

28 79. Plaintiff and the Class are “patients,” as defined in the CMIA, Cal. Civ.

1 Code § 56.05(l) (“‘Patient’ means a natural person, whether or not still living, who  
2 received health care services from a provider of healthcare and to whom medical  
3 information pertains.”).

4 80. Defendants disclosed “medical information,” as defined in the CMIA, Cal.  
5 Civ. Code § 56.05(i), to unauthorized persons without first obtaining consent, in  
6 violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized  
7 individuals in the Data Breach resulted from the inactions of Defendants, including  
8 their failure to adequately implement sufficient data security measures and protocols  
9 to protect Plaintiff’s and Class members’ personal and medical information, which  
10 allowed unauthorized individuals to obtain Plaintiff’s and the Class members’ medical  
11 information.

12 81. Defendants’ negligence resulted in the release of individually identifiable  
13 medical information pertaining to Plaintiff and the Class to unauthorized persons and  
14 the breach of the confidentiality of that information. Defendants’ negligent failure to  
15 maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff’s and Class  
16 members’ medical information in a manner that preserved the confidentiality of the  
17 information contained therein, was in violation of Cal. Civ. Code §§ 56.06 and  
18 56.101(a).

19 82. Defendants’ systems and protocols did not protect and preserve the  
20 integrity of electronic medical information in violation of Cal. Civ. Code §  
21 56.101(b)(1)(A).

22 83. Plaintiff and the Class were injured and have suffered damages, as  
23 described above, from Defendants’ illegal disclosure and negligent release of their  
24 medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore  
25 seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal  
26 statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and  
27 attorneys’ fees, expenses and costs.  
28

1 **Second Cause of Action**

2 **Negligence**

3 **[On Behalf of Plaintiff and the Class Against all Defendants]**

4 84. Plaintiff re-alleges and incorporates by reference each and every  
5 allegation contained in the preceding and subsequent paragraphs as though fully set  
6 forth herein.

7 85. Defendants' own negligent conduct created a foreseeable risk of harm to  
8 Plaintiff and Class members. Defendants' negligence included, but was not limited to,  
9 their failures to take the steps and opportunities to prevent the Data Breach as set  
10 forth herein. Defendants' negligence also included their decision not to comply with  
11 (1) industry standards, and/or best practices for the safekeeping and encrypted  
12 authorized disclosure of the Sensitive Information of Plaintiff and Class members; or  
13 (2) Section 5 of the FTC Act.

14 86. Defendants had a duty to exercise reasonable care in safeguarding,  
15 securing and protecting such information from being compromised, lost, stolen,  
16 misused, and/or disclosed to unauthorized parties. This duty includes, among other  
17 things, designing, maintaining and testing their security protocols to ensure Sensitive  
18 Information in Defendants' possession was adequately secured and protected, and  
19 that employees tasked with maintaining such information were adequately trained on  
20 relevant cybersecurity measures. Defendants also had a duty to put proper procedures  
21 in place to prevent the unauthorized dissemination of Plaintiff's and Class members'  
22 Sensitive Information.

23 87. Defendants' duty to use reasonable security measures under HIPAA  
24 required Defendants to "reasonably protect" confidential data from "any intentional  
25 or unintentional use or disclosure" and to "have in place appropriate administrative,  
26 technical, and physical safeguards to protect the privacy of protected health  
27 information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at  
28 issue in this case constitutes "protected health information" within the meaning of

1 HIPAA.

2 88. Plaintiff and the Class members entrusted their Sensitive Information to  
3 Defendants with the understanding that Defendants would safeguard their  
4 information.

5 89. Defendants were in a position to protect against the harm suffered by  
6 Plaintiff and Class members as a result of the Data Breach. However, Plaintiff and  
7 Class members had no ability to protect their Sensitive Information in Defendants'  
8 possession.

9 90. Defendants had full knowledge of the sensitivity of the Sensitive  
10 Information, and the types of harm Plaintiff and Class members could, would, and  
11 will suffer if the Sensitive Information were wrongfully disclosed.

12 91. Plaintiff and Class members were the foreseeable and probable victims of  
13 Defendants' negligent and inadequate security practices and procedures that led to the  
14 Data Breach. Defendants knew or should have known of the inherent risks in  
15 collecting and storing the highly valuable Sensitive Information of Plaintiff and Class  
16 members, the critical importance of providing adequate security of that Sensitive  
17 Information, the current cyber security risks being perpetrated, and that Defendants  
18 had inadequate employee training, monitoring and education and IT security  
19 protocols in place to secure the Sensitive Information of Plaintiff and Class members.

20 92. Defendants negligently, through their actions and/or omissions, and  
21 unlawfully breached their duty to Plaintiff and Class members by failing to exercise  
22 reasonable care in protecting and safeguarding Plaintiff's and Class members'  
23 Sensitive Information while the data was within Defendants' possession and/or  
24 control by failing to comply with and/or deviating from standard industry rules,  
25 regulations, and practices at the time of the Data Breach.

26 93. The harm the Data Breach caused is the type of harm privacy laws were  
27 intended to guard against. And Plaintiff and Class members are within the class of  
28 persons privacy laws were intended to protect.

1           94. Defendants negligently failed to comply with privacy laws by failing to  
2 protect against and prevent the dissemination of Plaintiff's and Class members'  
3 Sensitive Information to unauthorized third parties.

4           95. Defendants' violations of Section 5 of the FTC Act also constitute  
5 negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting  
6 commerce," including, as interpreted and enforced by the FTC, the unfair act or  
7 practice by businesses, such as Defendants, of failing to use reasonable measures to  
8 protect Sensitive Information. The FTC publications and orders described above also  
9 form part of the basis of Defendants' duty in this regard.

10          96. Defendants violated Section 5 of the FTC Act by failing to use reasonable  
11 measures to protect Plaintiff's and Class members' Sensitive Information and not  
12 complying with applicable industry standards, as described in detail herein.  
13 Defendants' conduct was particularly unreasonable given the nature and amount of  
14 Sensitive Information they required, obtained, and stored, and the foreseeable  
15 consequences of a data breach including, specifically, the damages that would result  
16 to Plaintiff and Class members.

17          97. Plaintiff and Class members are within the class of persons the FTC Act  
18 was intended to protect.

19          98. The harm the Data Breach caused, and continues to cause, is the type of  
20 harm the FTC Act was intended to guard against. The FTC pursues enforcement  
21 actions against businesses, which, as a result of their failure to employ reasonable  
22 data security measures and avoid unfair and deceptive practices, caused the same  
23 harm as that suffered by Plaintiff and Class members.

24          99. Defendants, through their actions and/or omissions, unlawfully breached  
25 their duty to Plaintiff and Class members by failing to have appropriate procedures in  
26 place to detect and prevent unauthorized dissemination of Plaintiff's and Class  
27 members' Sensitive Information.

28          100. Defendants, through their actions and/or omissions, unlawfully breached

1 their duty to adequately disclose to Plaintiff and Class members the existence and  
2 scope of the Data Breach.

3 101. But for Defendants' wrongful and negligent breach of duties owed to  
4 Plaintiff and Class members, Plaintiff's and Class members' Sensitive Information  
5 would not have been compromised.

6 102. There is a temporal and close causal connection between Defendants'  
7 failure to implement security measures to protect the Sensitive Information and the  
8 harm suffered, and/or risk of imminent harm suffered, by Plaintiff and Class  
9 members.

10 103. As a direct and proximate result of Defendants' negligence, Plaintiff and  
11 Class members have suffered, and continue to suffer, injuries and damages arising  
12 from the Data Breach, including, but not limited to: damages from lost time and  
13 efforts to mitigate the actual and potential impact of the Data Breach on their lives,  
14 including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies,  
15 contacting their financial institutions, closing or modifying financial accounts, closely  
16 reviewing and monitoring their credit reports and various accounts for unauthorized  
17 activity, filing police reports, and damages from identity theft, which may take  
18 months—if not years—to discover, detect, and remedy.

19 104. Additionally, as a direct and proximate result of Defendants' negligence,  
20 Plaintiff and Class members have suffered, and will continue to suffer, the continued  
21 risks of exposure of their Sensitive Information, which remains in Defendants'  
22 possession and is subject to further unauthorized disclosures so long as Defendants  
23 fail to undertake appropriate and adequate measures to protect the Sensitive  
24 Information in their continued possession.

1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

4  
5  
6  
7  
8  
9  
0  
1  
2  
3  
4  
5  
6  
7  
8

0  
1  
2  
3  
4  
5  
6  
7  
8

4  
5  
6  
7  
8

1 112. Acting with knowledge, Defendants had notice and knew that their  
2 inadequate cybersecurity practices would cause injury to Plaintiff and Class  
3 members.

4 113. As a proximate result of Defendants' acts and omissions, Plaintiff and  
5 Class members' Sensitive Information was disclosed to, and used by, third parties  
6 without authorization, causing Plaintiff and Class members to suffer damages.

7 114. Unless and until enjoined and restrained by order of this Court,  
8 Defendants' wrongful conduct will continue to cause great and irreparable injury to  
9 Plaintiff and Class members in that the Sensitive Information maintained by  
10 Defendants may be breached again—leading to further viewing, distributing, and use  
11 of updated and additional Sensitive Information by unauthorized persons.

12 115. Plaintiff and Class members have no adequate remedy at law for the  
13 injuries in that a judgment for monetary damages will not end the invasion of privacy  
14 for Plaintiff and Class members.

15 **Fourth Cause of Action**

16 **Breach of Implied Contract**

17 **[On Behalf of Plaintiff and the Class Against all Defendants]**

18 116. Plaintiff re-alleges and incorporates by reference each and every  
19 allegation contained in the preceding and subsequent paragraphs as though fully set  
20 forth herein.

21 117. Defendants solicited and invited Class members to provide their Sensitive  
22 Information as part of Defendants' regular business practices. Plaintiff and Class  
23 members provided their Sensitive Information to Defendants.

24 118. In so doing, Plaintiff and Class members entered into implied contracts  
25 with Defendants pursuant to which Defendants agreed to safeguard and protect such  
26 information and to timely detect any breaches of their Sensitive Information. In  
27 entering into such implied contracts, Plaintiff and Class members reasonably believed  
28

1 and expected that Defendants' data security practices complied with relevant laws  
2 and regulations, including HIPAA, and were consistent with industry standards.

3 119. Implicit in the agreement between Plaintiff and Class members on the one  
4 hand, and the Defendants on the other, regarding providing protected Sensitive  
5 Information, was Defendants' obligation to: (a) use such Sensitive Information for  
6 business purposes only; (b) take reasonable steps to safeguard that Sensitive  
7 Information; (c) prevent unauthorized disclosures of the Sensitive Information;  
8 (d) provide Plaintiff and Class members with prompt and sufficient notice of any and  
9 all unauthorized access and/or theft of their Sensitive Information; (e) reasonably  
10 safeguard and protect the Sensitive Information of Plaintiff and Class members from  
11 unauthorized disclosure or uses; and (f) retain the Sensitive Information only under  
12 conditions that kept such information secure and confidential.

13 120. Without such implied contracts, Plaintiff and Class members would not  
14 have provided their Sensitive Information to Defendants.

15 121. Plaintiff and Class members fully performed their obligations under the  
16 implied contract with Defendants. However, Defendants did not.

17 122. Defendants breached the implied contracts with Plaintiff and Class  
18 members by failing to:

19 a. Reasonably safeguard and protect Plaintiff's and Class members'  
20 Sensitive Information, which was compromised as a result of the Data  
21 Breach; and

22 b. Identify and respond to suspected or known security incidents.

23 123. As a direct and proximate result of Defendants' breach of the implied  
24 contracts, Plaintiff and Class members have suffered, and continue to suffer, injuries  
25 and damages arising from the Data Breach including, but not limited to: damages  
26 from lost time and effort to mitigate the actual and potential impact of the Data  
27 Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with  
28 credit reporting agencies, contacting their financial institutions, closing or modifying

1 financial accounts, closely reviewing and monitoring their credit reports and various  
2 accounts for unauthorized activity, filing police reports, and damages from identity  
3 theft, which may take months if not years to discover, detect, and remedy.

4 **Fifth Cause of Action**

5 **Breach of Fiduciary Duty**

6 **[On Behalf of Plaintiff and the Class Against all Defendants]**

7 124. Plaintiff re-alleges and incorporates by reference each and every  
8 allegation contained in the preceding and subsequent paragraphs as though fully set  
9 forth herein.

10 125. In light of their special relationship, Defendants became the guardian of  
11 Plaintiff's and Class members' Sensitive Information. Defendants became a  
12 fiduciary, created by their undertaking and guardianship of Plaintiff's and Class  
13 members' Sensitive Information, to act primarily for the benefit of Plaintiff and Class  
14 members. This duty included the obligation to safeguard Plaintiff's and Class  
15 members' Sensitive Information, and to timely notify them in the event of a data  
16 breach.

17 126. Defendants have a fiduciary duty to act for the benefit of Plaintiff and  
18 Class members upon matters within the scope of their relationship. Defendants  
19 breached their fiduciary duties owed to Plaintiff and Class members by failing to:

- 20 a. Properly encrypt and otherwise protect the integrity of the system  
21 containing Plaintiff's and Class members' protected confidential  
22 information and other Sensitive Information;  
23 b. Timely notify and/or warn Plaintiff and Class members of the Data  
24 Breach; and  
25 c. Otherwise failing to safeguard Plaintiff's and Class members' Sensitive  
26 Information.

27 127. As a direct and proximate result of Defendants' breaches of their  
28 fiduciary duties, Plaintiff and Class members have suffered, and will suffer, injury,

1 including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to  
2 control how their Sensitive Information is used; (c) the compromise, publication,  
3 and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with  
4 the prevention, detection, and recovery from identity theft and/or unauthorized use of  
5 their Sensitive Information; (e) lost opportunity costs associated with the effort  
6 expended and the loss of productivity addressing and attempting to mitigate the actual  
7 and future consequences of the Data Breach, including but not limited to efforts spent  
8 researching how to prevent, detect, contest, and recover from identity theft; (f) the  
9 continued risk to their Sensitive Information, which remain in Defendants' possession  
10 and is subject to further unauthorized disclosures so long as Defendants fail to  
11 undertake appropriate and adequate measures to protect the Sensitive Information in  
12 continued possession; and (g) future costs in terms of time, effort, and money that  
13 will be expended to prevent, detect, contest, and repair the impact of the Sensitive  
14 Information compromised as a result of the Data Breach for the remainder of the lives  
15 of Plaintiff and Class members.

16 128. As a direct and proximate result of Defendants' breach of their fiduciary  
17 duties, Plaintiff and Class members have suffered, and will continue to suffer, other  
18 forms of injury and/or harm, and other economic and non-economic losses.

19 **Sixth Cause of Action**

20 **Breach of Confidence**

21 **[On Behalf of Plaintiff and the Class Against all Defendants]**

22 129. Plaintiff re-alleges and incorporates by reference each and every  
23 allegation contained in the preceding and subsequent paragraphs as though fully set  
24 forth herein.

25 130. At all times during Plaintiff's and Class members' interactions with  
26 Defendants, Defendants were fully aware of the confidential and sensitive nature of  
27 Plaintiff's and Class members' Sensitive Information that Plaintiff and Class  
28 members provided to Defendants.

1           131. As alleged herein and above, Defendants' relationship with Plaintiff and  
2 Class members was governed by terms and expectations that Plaintiff's and Class  
3 members' Sensitive Information would be collected, stored, and protected in  
4 confidence, and would not be disclosed to unauthorized third parties.

5           132. Plaintiff and Class members provided their respective Sensitive  
6 Information to Defendants with the explicit and implicit understandings that  
7 Defendants would protect and not permit the Sensitive Information to be  
8 disseminated to any unauthorized parties.

9           133. Plaintiff and Class members also provided their Sensitive Information to  
10 Defendants with the explicit and implicit understandings that Defendants would take  
11 precautions to protect that Sensitive Information from unauthorized disclosure, such  
12 as following basic principles of protecting their networks and data systems, including  
13 Defendants' employees' systems.

14           134. Defendants required and voluntarily received, in confidence, Plaintiff's  
15 and Class members' Sensitive Information with the understanding that the Sensitive  
16 Information would not be disclosed or disseminated to the public or any unauthorized  
17 third parties.

18           135. Due to Defendants' failure to prevent, detect, and avoid the Data Breach  
19 from occurring by, *inter alia*, following best information security practices to secure  
20 Plaintiff's and Class members' Sensitive Information, Plaintiff's and Class members'  
21 Sensitive Information was disclosed to, and misappropriated by, unauthorized third  
22 parties beyond Plaintiff's and Class members' confidence, and without their express  
23 permission.

24           136. As a direct and proximate cause of Defendants' actions and/or omissions,  
25 Plaintiff and Class members have suffered, and will continue to suffer damages.

26           137. But for Defendants' disclosure of Plaintiff's and Class members'  
27 Sensitive Information in violation of the parties' understanding of confidence,  
28 Plaintiff's and Class members' Sensitive Information would not have been

1 compromised, stolen, viewed, accessed, and used by unauthorized third parties.

2 Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and  
3 Class members' Sensitive Information, as well as the resulting damages.

4 138. The injury and harm Plaintiff and Class members suffered, and continue  
5 to suffer, was the reasonably foreseeable result of Defendants' unauthorized  
6 disclosure of Plaintiff's and Class members' Sensitive Information. Defendants knew  
7 that their computer systems and technologies for accepting and securing Plaintiff's  
8 and Class members' Sensitive Information had numerous security and other  
9 vulnerabilities placing Plaintiff's and Class members' Sensitive Information in  
10 jeopardy.

11 139. As a direct and proximate result of Defendants' breaches of confidence,  
12 Plaintiff and Class members have suffered and will suffer injury, including but not  
13 limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of  
14 their Sensitive Information; (c) out-of-pocket expenses associated with the  
15 prevention, detection, and recovery from identity theft and/or unauthorized use of  
16 their Sensitive Information; (d) lost opportunity costs associated with effort expended  
17 and the loss of productivity addressing and attempting to mitigate the actual and  
18 future consequences of the Data Breach, including but not limited to efforts spent  
19 researching how to prevent, detect, contest, and recover from identity theft; (e) the  
20 continued risk to their Sensitive Information, which remains in Defendants'  
21 possession and is subject to further unauthorized disclosures so long as Defendants  
22 fail to undertake appropriate and adequate measures to protect the Sensitive  
23 Information in their continued possession; (f) future costs in terms of time, effort, and  
24 money that will be expended as result of the Data Breach for the remainder of the  
25 lives of Plaintiff and Class members; and (g) the diminished value of Defendants'  
26 services they received.

27 140. As a direct and proximate result of Defendants' breaches of their  
28 fiduciary duties, Plaintiff and Class members have suffered and will continue to

1 suffer other forms of injury and/or harm, and other economic and non-economic  
2 losses.

3 **Seventh Cause of Action**

4 **Violation of the California Unfair Competition Law,**

5 **Cal. Bus. & Prof. Code § 17200, *et seq.*--Unfair Business Practices**

6 **[On Behalf of Plaintiff and the California Subclass Against all Defendants]**

7 141. Plaintiff re-alleges and incorporates by reference each and every  
8 allegation contained in the preceding and subsequent paragraphs as though fully set  
9 forth herein.

10 142. Defendants violated Cal. Bus. & Prof. Code § 17200, *et seq.*, by engaging  
11 in unlawful, unfair, or fraudulent business acts and practices, that constitute acts of  
12 “unfair competition” as defined in Cal. Bus. & Prof. Code § 17200.

13 143. Defendants engaged in unlawful and unfair acts and practices by  
14 establishing the sub-standard security practices and procedures described herein; by  
15 soliciting and collecting Plaintiff’s and Class members’ Sensitive Information with  
16 knowledge the information would not be adequately protected; and by storing  
17 Plaintiff’s and Class members’ Sensitive Information in an unsecure electronic  
18 environment in violation of California’s data breach statute, Cal. Civ. Code §  
19 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the  
20 Sensitive Information of Plaintiff and Class members.

21 144. In addition, Defendants engaged in unlawful acts and practices by failing  
22 to disclose the Data Breach in a timely and accurate manner, contrary to the duties  
23 imposed by Cal. Civ. Code § 1798.82.

24 145. Defendants also engaged in unlawful acts by violating the privacy and  
25 security of HIPAA, 42 U.S.C. §1302d, *et seq.* and by violating the CMIA, Cal. Civ.  
26 Code § 56, *et seq.*

27 146. Defendants’ practices were also contrary to legislatively declared and  
28 public policies that seek to protect consumer data and ensure that entities that solicit

1 or are entrusted with personal data utilize appropriate security measures, as reflected  
2 by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., and  
3 the CMIA, Cal. Civ. Code § 56, et seq.

4 147. As a direct and proximate result of Defendants' unlawful and unfair  
5 practices and acts, Plaintiff and Class members were injured and lost money or  
6 property, including but not limited to the loss of Plaintiff's and Class members'  
7 legally protected interest in the confidentiality and privacy of their Sensitive  
8 Information, nominal damages, and additional losses as described herein.

9 148. Defendants knew or should have known that their computer systems and  
10 data security practices were inadequate to safeguard Plaintiff's and Class members'  
11 Sensitive Information and that the risk of a data breach or theft was highly likely.  
12 Defendants' actions in engaging in the above-named unlawful practices and acts  
13 were negligent, knowing, and willful, and/or wanton and reckless with respect to the  
14 rights of Plaintiff and Class members.

15 149. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code  
16 § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class  
17 members of money or property Defendants may have acquired by means of  
18 Defendants' unlawful, and unfair business practices, restitutionary disgorgement of  
19 all monies that accrued to Defendants because of Defendants' unlawful and unfair  
20 business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code  
21 Civ. Proc. § 1021.5), and injunctive or other equitable relief.

### 22 **Eighth Cause of Action**

#### 23 **Violation of the California Customer Records Act ("CCRA")**

#### 24 **Cal. Civ. Code § 1798.80, *et seq.***

#### 25 **[On Behalf of Plaintiff and the California Subclass Against all Defendants]**

26 150. Plaintiff re-alleges and incorporates by reference each and every  
27 allegation contained in the preceding and subsequent paragraphs as though fully set  
28 forth herein.

1           151. Section 1798.82 of the California Civil Code requires any “person or  
2 business that conducts business in California, and that owns or licenses computerized  
3 data that includes personal information” to “disclose any breach of the security of the  
4 system following discovery or notification of the breach in the security of the data to  
5 any resident of California whose unencrypted personal information was, or is  
6 reasonably believed to have been, acquired by an unauthorized person.” Under  
7 section 1798.82, the disclosure “shall be made in the most expedient time possible  
8 and without unreasonable delay.”

9           152. The CCRA further provides: “Any person or business that maintains  
10 computerized data that includes personal information that the person or business does  
11 not own shall notify the owner or licensee of the information of any breach of the  
12 security of the data immediately following discovery, if the personal information was,  
13 or is reasonably believed to have been, acquired by an unauthorized person.” (Cal.  
14 Civ. Code § 1798.82(b).)

15           153. Any person or business required to issue a security breach notification  
16 under the CCRA shall meet the following requirements:

- 17           a. The security breach notification shall be written in plain language;
- 18           b. The security breach notification shall include, at a minimum, the  
19           following information:
  - 20           i. The name and contact information of the reporting person or  
21           business subject to this section;
  - 22           ii. A list of the types of personal information that were or are  
23           reasonably believed to have been the subject of a breach;
  - 24           iii. If the information is possible to determine at the time the  
25           notice is provided, then any of the following:
    - 26           1. The date of the breach;
    - 27           2. The estimated date of the breach; or

- 1                   3. The date range within which the breach occurred. The  
2                   notification shall also include the date of the notice.
- 3                   iv. Whether notification was delayed as a result of a law  
4                   enforcement investigation, if that information is possible to  
5                   determine at the time the notice is provided;
- 6                   v. A general description of the breach incident, if that information  
7                   is possible to determine at the time the notice is provided; and
- 8                   vi. The toll-free telephone numbers and addresses of the major  
9                   credit reporting agencies if the breach exposed a Social  
10                  Security number or a driver's license or California  
11                  identification card number.

12               154. The Data Breach described herein constituted a “breach of the security  
13 system” of Defendants.

14               155. As alleged above, Defendants unreasonably delayed informing Plaintiff  
15 and Class members about the Data Breach, affecting their Sensitive Information, after  
16 Defendants knew the Data Breach had occurred.

17               156. Defendants failed to disclose to Plaintiff and Class members, without  
18 unreasonable delay and in the most expedient time possible, the breach of security of  
19 their unencrypted, or not properly and securely encrypted, Sensitive Information  
20 when Defendants knew or reasonably believed such information had been  
21 compromised.

22               157. Defendants’ ongoing business interests gave Defendants incentive to  
23 conceal the Data Breach from the public to ensure continued revenue.

24               158. Upon information and belief, no law enforcement agency instructed  
25 Defendants that timely notification to Plaintiff and Class members would impede  
26 their investigation.

27               159. As a result of Defendants’ violation of Cal. Civ. Code § 1798.82, Plaintiff  
28 and Class members were deprived of prompt notice of the Data Breach, and were

1 thus prevented from taking appropriate protective measures, such as securing identity  
2 theft protection or requesting a credit freeze. These measures could have prevented  
3 some of the damages suffered by Plaintiff and Class members because their stolen  
4 information would have had less value to identity thieves.

5 160. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiff  
6 and Class members suffered incrementally increased damages separate and distinct  
7 from those simply caused by the Data Breach itself.

8 161. Plaintiff and Class members seek all remedies available under Cal. Civ.  
9 Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and  
10 Class members as alleged above and equitable relief.

11 **Ninth Cause of Action**

12 **Violation of the California Consumer Privacy Act ("CCPA")**

13 **Cal. Civ. Code § 1798.150, *et seq.***

14 **[On Behalf of Plaintiff and the California Subclass Against all Defendants]**

15 162. Plaintiff re-alleges and incorporates by reference each and every  
16 allegation contained in the preceding and subsequent paragraphs as though fully set  
17 forth herein.

18 163. Defendants are corporations organized and operated for profit or financial  
19 benefit of their owners with annual gross revenues of more than \$25 million.  
20 Defendants collect consumers' PII as defined in Cal. Civ. Code § 1798.140.

21 164. Defendants violated § 1798.150 of the CCPA by failing to prevent  
22 Plaintiff's and Class members' nonencrypted PII from unauthorized access and  
23 exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to  
24 implement and maintain reasonable security procedures and practices appropriate to  
25 the nature of the information.

26 165. Defendants have a duty to implement and maintain reasonable security  
27 procedures and practices to protect Plaintiff's and Class members' PII. As detailed  
28 herein, Defendants failed to do so. As a direct and proximate result of Defendants'

1 acts, Plaintiff's and Class members' PII were subjected to unauthorized access and  
2 exfiltration, theft or disclosure.

3 166. Plaintiff and Class members seek injunctive or other equitable relief to  
4 ensure Defendants hereinafter adequately safeguard consumers' PII by implementing  
5 reasonable security procedures and practices. Such relief is particularly important  
6 because Defendants continue to hold consumers' PII including Plaintiff's and Class  
7 members' PII. Plaintiff and Class members have an interest in ensuring that their PII  
8 is reasonably protected, and Defendants have demonstrated a pattern of failing to  
9 adequately safeguard this information.

### 10 **PRAYER FOR RELIEF**

11 **WHEREFORE**, Plaintiff prays for judgment as follows:

- 12 1. That the Court certify this action as a Class Action under FRCP 23 and  
13 appoint Plaintiff as representative of the Class and his attorneys as Class  
14 Counsel;
- 15 2. Granting injunctive relief requested by Plaintiff, including but not  
16 limited to, injunctive and other equitable relief as is necessary to protect  
17 the interests of Plaintiff and Class members, including but not limited to  
18 an order:
  - 19 i. prohibiting Defendants from engaging in the wrongful and  
20 unlawful acts described herein,
  - 21 ii. requiring Defendants to protect, including through encryption, all  
22 data collected through the course of their business in accordance  
23 with all applicable regulations, industry standards, and federal,  
24 state or local laws,
  - 25 iii. requiring Defendants to delete, destroy, and purge the personal  
26 information of Plaintiff and Class members unless Defendants can  
27 provide to the Court reasonable justification for the retention and  
28 use of such information when weighed against the privacy

- 1 interests of Plaintiff and Class members,
- 2 iv. requiring Defendants to implement and maintain a comprehensive
- 3 Information Security Program designed to protect the
- 4 confidentiality and integrity of Plaintiff and Class members’
- 5 personal information,
- 6 v. prohibiting Defendants from maintaining Plaintiff’s and Class
- 7 members’ personal information on a cloud-based database,
- 8 vi. requiring Defendants to engage independent third-party security
- 9 auditors/penetration testers as well as internal security personnel
- 10 to conduct testing, including simulated attacks, penetration tests,
- 11 and audits on Defendants’ systems on a periodic basis, and
- 12 ordering Defendants to promptly correct any problems or issues
- 13 detected by such third-party security auditors,
- 14 vii. requiring Defendants to engage independent third-party security
- 15 auditors and internal personnel to run automated security
- 16 monitoring,
- 17 viii. requiring Defendants to audit, test, and train their security
- 18 personnel regarding any new or modified procedures,
- 19 ix. requiring Defendants to conduct regular database scanning and
- 20 security checks,
- 21 x. requiring Defendants to establish an information security training
- 22 program that includes at least annual information security training
- 23 for all employees, with additional training to be provided as
- 24 appropriate based upon the employees’ respective responsibilities
- 25 with handling personal information, as well as protecting the
- 26 personal information of Plaintiff and Class members,
- 27 xi. requiring Defendants to routinely and continually conduct internal
- 28 training and education, and on an annual basis to inform internal

- 1 security personnel how to identify and contain a breach when it  
2 occurs and what to do in response to a breach,
- 3 xii. requiring Defendants to implement a system of tests to assess their  
4 respective employees' knowledge of the education programs  
5 discussed in the preceding subparagraphs, as well as randomly and  
6 periodically testing employees' compliance with Defendants'  
7 policies, programs, and systems for protecting personal  
8 information,
- 9 xiii. requiring Defendants to implement, maintain, regularly review, and  
10 revise as necessary a threat management program designed to  
11 appropriately monitor Defendants' information networks for  
12 threats, both internal and external, and assess whether monitoring  
13 tools are appropriately configured, tested, and updated,
- 14 xiv. requiring Defendants to meaningfully educate all Class members  
15 about the threats that they face as a result of the loss of their  
16 confidential personal information to third parties, as well as the  
17 steps affected individuals must take to protect themselves,
- 18 xv. requiring Defendants to design, maintain, and test their computer  
19 systems to ensure that PII in their possession is adequately secured  
20 and protected,
- 21 xvi. requiring Defendants to disclose any future data disclosures in a  
22 timely and accurate manner; and
- 23 xvii. requiring Defendants to provide ongoing credit monitoring and  
24 identity theft repair services to Class members.
- 25 3. An award of compensatory, statutory, and nominal damages in an amount to  
26 be determined;
- 27 4. An award for equitable relief requiring restitution and disgorgement of the  
28 revenues wrongfully retained as a result of Defendants' wrongful conduct;

